HONOLULU POLICE DEPARTMENT

POLICY
AUXILIARY AND TECHNICAL SERVICES

November 14, 2019	Policy Number 8.20

COMPUTER SECURITY

POLICY

To outline the responsibilities of departmental personnel for the use of city and county workstations, desktop computers, laptops, and/or other portable computer devices.

PROCEDURE

I. DEFINITIONS

A. Information systems: Any combination of hardware and software used to collect, process, store, and disseminate data.

B. User identifier: Credentials, such as a user name, which are used to verify the individual and the individual's access to an information system.

II. RESPONSIBILITIES

A. General Responsibilities

The Honolulu Police Department (HPD) security administrator(s) oversees information systems for the department and all agencies that have been given access to the HPD systems. Each element security liaison oversees all users within the element. Users are responsible for maintaining the confidentiality, integrity, and availability of the systems.

B. HPD Security Administrator(s)

The commander of the Information Technology Division (ITD) shall appoint the HPD security administrator(s) whose responsibilities to the division commander include the following:

1. Formulating and implementing policy and procedures relating to the security of the systems;

2. Controlling and monitoring the HPD information systems to ensure the confidentiality, integrity, and availability of the systems;

3. Coordinating with outside agencies who have authorization from the Chief of Police to access the HPD information systems;

4. Investigating and/or assisting in security violation investigations and recommending corrective measures; and

5. Coordinating new developments and changes in security procedures with element security liaisons.

C. Element Security Liaisons

Division-level commanders shall appoint element security liaisons whose responsibilities include the following:

1. Instructing authorized users in their element on computer procedures;

2 Designating and verifying authorized users in the element and defining and modifying access as required;

3. Assisting in the investigation of security violations;

4. Providing training for replacement element security liaisons and keeping the HPD security administrator(s) apprised of the current element security liaison(s); and

5. Agreeing to be the custodians of the equipment issued by acknowledging written receipt of desktop computers, workstations, or laptops and any or all components in writing prior to their intended use.

D. Authorized Users

Authorized users shall:

1. Utilize information systems and equipment for official work-related purposes only;

2. Remain cognizant of computer security procedures to ensure the confidentiality, integrity, and availability of the systems. All credentials, including user identifiers and passwords, shall be safeguarded;

3. Report violations of computer security procedures to the element security liaisons;

4. Ensure that the equipment is properly secured if left unattended, including locking computers left unattended for more than 30 minutes;

5. Report any lost or stolen equipment;

6. Attempt to access only the resources that are defined in an individual's profile;

7. Use only authorized information obtained from an information system. The unauthorized release of confidential information may be a violation of the privacy act; and

8. Receive prior written authorization from the commander or designee of the ITD before taking any city-owned computer or computer-related equipment, such as air cards, data storage devices, etc., out of the United States of America.

III. PASSWORD RESETS

A. During normal business hours, password resets shall be requested by [redacted]

B. If a password reset is required immediately during nonbusiness hours, the requestor shall [redacted]

John D. McCarthy

for SUSAN BALLARD
Chief of Police

Post on bulletin
board for one week